

WHAT IS CLAIMED IS:

1 1. A method for preventing packet retransmissions during Internet Protocol security (IPsec)
2 security association establishment comprising:

3 monitoring application socket requests;
4 requesting a Transmission Control Protocol (TCP) connection by an application;
5 determining if there is an active security association that exists to protect network flow
6 associated with the connection request;

7 preventing the connection request from proceeding if no active security association exists to
8 protect the network flow;

9 determining if a security policy exists for the network flow if no active security association
10 exists to protect the network flow;

11 alerting a security association negotiation component to initiate negotiation for a security
12 association based on the security policy if the security policy exists for the network flow; and

13 allowing the connection request to proceed if one of the active security association exists and
14 the security association is established from the negotiation.

1 2. The method according to claim 1, wherein the security association negotiation component
2 comprises an Internet Key Exchange (IKE) component.

1 3. The method according to claim 1, wherein the active security association and the security
2 association are based on at least one of a source Internet Protocol (IP) address, a destination IP
3 address, a protocol, a source port, and a destination port.

1 4. The method according to claim 3, wherein the protocol comprises one of TCP, User
2 Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and Internet Group
3 Management Protocol (IGMP).

1 5. The method according to claim 1, further comprising determining if the network flow can
2 be allowed without a security association if no security policy exists for the network flow.

1 6. The method according to claim 1, further comprising retrieving the security association
2 from a database.

1 7. The method according to claim 6, wherein the database contains mappings between
2 network flow information and security associations.

1 8. The method according to claim 7, wherein the network flow information comprises at least
2 one of a source Internet Protocol (IP) address, a destination IP address, a protocol, a source port,
3 and a destination port.

1 9. The method according to claim 1, further comprising retrieving the security policy from
2 a database.

1 10. A method for preventing packet retransmissions during Internet Protocol security (IPsec)
2 security association establishment comprising:
3 monitoring application socket requests;
4 requesting transmission of User Datagram Protocol (UDP) data on a socket by the
5 application;
6 determining if the socket has been associated with an active security association;
7 determining if there is a defined security association that may be used to protect network flow
8 if the socket has not been associated with an active security association;
9 determining what security policy should be used when negotiating a security association for
10 the network flow if there is no defined security association that may be used to protect the
11 network flow;
12 alerting a security association negotiation component to initiate negotiation for the security
13 association if there is no defined security association that may be used to protect the network
14 flow;
15 establishing the security association; and
16 allowing the UDP data to be sent.

1 11. The method according to claim 10, wherein the security association negotiation
2 component comprises an Internet Key Exchange (IKE) component.

1 12. The method according to claim 10, comprising negotiating for a security association
2 using security parameters specified by a policy.

1 13. The method according to claim 10, wherein the second determining comprises comparing
2 filters with at least one of a source Internet Protocol (IP) address, a destination IP address, a
3 protocol, a source port, and a destination port, the at least one of a source Internet Protocol (IP)
4 address, a destination IP address, a protocol, a source port, and a destination port related to the
5 network flow, the filters related to defined security associations.

14. The method according to claim 13, each filter comprising at least one of a source Internet
Protocol (IP) address, a destination IP address, a protocol, a source port, and a destination port.

15. The method according to claim 13, wherein the security policy comprises at least one
filter.

16. The method according to claim 10, further comprising determining if the network flow
can be allowed without a security association if no security policy exists for the network flow.

1 17. A computing device for preventing packet retransmissions during Internet Protocol
2 security (IPsec) security association establishment with a network unit, the device and network
3 unit operably connected to a network, the computing device comprising:

4 a network interceptor, the network interceptor monitoring an application's socket requests;

5 a security association database operably connected to the network interceptor, the security
6 association database containing a mapping of network flow information to security association
7 information;

8 a security policy database operably connected to the network interceptor, the security policy
9 database containing policies that describe parameters that are to be used in a negotiation of a
10 security association;

11 a security association negotiation component, the security association negotiation component
12 operably connected to the network interceptor, the security association negotiation component
13 capable of negotiating a security association with a network unit; and

14 an Internet Protocol security (IPsec) packet classifier, the IPsec packet classifier responsible
15 for performing IPsec processing on incoming and outgoing packets,

16 wherein the network interceptor insures that a security association is in place before allowing
17 network traffic to flow between the application and the network unit.

18 18. The device according to claim 17, wherein the network flow information comprises at
19 least one of Internet Protocol (IP) addresses, protocol, and ports.

20 19. The device according to claim 17, wherein the security association negotiation
21 component comprises Internet Key Exchange (IKE).

22 20. An article comprising a storage medium having instructions stored therein, when
23 executed causes a computing device to perform:

3 monitoring application socket requests;
4 requesting a Transmission Control Protocol (TCP) connection by an application;
5 determining if there is an active security association that exists to protect network flow
6 associated with the connection request;
7 preventing the connection request from proceeding if no active security association exists to
8 protect the network flow;
9 determining if a security policy exists for the network flow if no active security association
10 exists to protect the network flow;
11 alerting a security association negotiation component to initiate negotiation for a security
12 association based on the security policy if the security policy exists for the network flow; and
13 allowing the connection request to proceed if one of the active security association exists and
14 the security association is established from the negotiation.

21. The article according to claim 20, wherein the security association negotiation
2 component comprises an Internet Key Exchange (IKE) component.

1 22. The article according to claim 20, comprising negotiating for a security association using
2 security parameters specified by a policy.

1 23. The article according to claim 20, wherein the active security association comprises at
2 least one of source Internet Protocol (IP), destination IP, protocol, source port, and destination
3 port.

1 24. An article comprising a storage medium having instructions stored therein, the
2 instructions when executed causes a computing device to perform:

3 monitoring application socket requests;

4 requesting transmission of User Datagram Protocol (UDP) data on a socket by the
5 application;

6 determining if the socket has been associated with an active security association;

7 determining if there is a defined security association that may be used to protect network flow
8 if the socket has not been associated with an active security association;

9 determining what security policy should be used when negotiating a security association for
10 the network flow if there is no defined security association that may be used to protect the
11 network flow;

12 alerting a security association negotiation component to initiate negotiation for the security
13 association if there is no defined security association that may be used to protect the network
14 flow;

15 establishing the security association; and

16 allowing the UDP data to be sent.

1 25. The article according to claim 24, wherein the security association negotiation
2 component comprises an Internet Key Exchange (IKE) component.

1 26. The article according to claim 24, comprising negotiating for a security association using
2 security parameters specified by a policy.

1 27. The article according to claim 24, wherein the active security association comprises at
2 least one of source Internet Protocol (IP), destination IP, protocol, source port, and destination
3 port.

1 28. A method for preventing packet retransmissions during Internet Protocol security (IPsec)
2 security association establishment comprising:

3 monitoring application socket requests;

4 requesting a Transmission Control Protocol (TCP) connection by an application;

5 determining if there is an active security association that exists to protect network flow
6 associated with the connection request;

7 determining if a security policy exists for the network flow if no active security association
8 exists to protect the network flow;

9 alerting a security association negotiation component to initiate negotiation for a security
10 association based on the security policy if the security policy exists for the network flow; and

11 allowing the connection request to proceed if one of the active security association exists and
12 the security association is established from the negotiation.

- 1 29. The method according to claim 28, further comprising preventing the connection request
- 2 from proceeding if no active security association exists to protect the network flow after the first
- 3 determining.

00ET90" T4826560